IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

First Named Inventor: Adam R. Schran		:	
Conf. No.:	3079	:	Group Art Unit: 2161
Appln. No.:	09/820,054	:	Examiner: Etienne Pierre Leroux
Filing Date:	March 28, 2001	:	Attorney Docket No.: 10397-1U1
Title:	SYSTEM AND METHOD FOR NETWORK ADMINISTRATION AND LOCAL ADMINISTRATION OF PRIVACY PROTECTION CRITERIA	:	

4th AMENDED APPEAL BRIEF (37 C.F.R. § 41.37)

This brief is being timely filed in response to the "Notification of Non-Compliant Appeal Brief mailed January 27, 2009. No extension of time fees are due. The fees required under § 41.20 were paid when the original Appeal Brief was filed and no additional appeal-related fees are believed to be due. However, if any fees are due, charge them to Deposit Acct. No. 50-1017.

The following non-substantive changes were made in this amended Appeal Brief:

1. Section VIID. ARGUMENTS – REJECTIONS UNDER 35 U.S.C. § 103 now includes separate headings in accordance with 37 CFR 41.37(c)(1)(viii) that match Section VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL. See PARTS 1 and 2 of Section VIID.

2. A revised Table of Contents is provided.

To avoid any confusion regarding the contents of the appeal brief, especially in view of the previously filed 3rd Amended Appeal Brief that included only a revised portion of Section V of the 2nd Amended Appeal Brief, the entire appeal brief was resubmitted which incorporates the changes made in the 3rd Amended Appeal Brief. No substantive changes were made to the last version of the appeal brief.

This brief is being filed in response to the non-final Office Action dated March 18, 2008 and supersedes the three previously filed Appeal Briefs. Although the outstanding Office Action is non-final, the claims have been twice rejected, and thus an immediate filing of this Appeal Brief is permissible. The fees required under § 41.20 were paid when the original Appeal Brief was filed and thus no additional fees are believed to be due.

The comments in Reply Brief filed on September 11, 2008 should still be considered in conjunction with this consolidated 4th Amended Appeal Brief.

TABLE OF CONTENTS

I. REAL PARTY IN INTEREST

This application is assigned to Ascentive LLC, by an Assignment recorded on March 28, 2001, at Reel No. 011662, Frame 0557. Accordingly, Ascentive LLC is the real party in interest.

II. RELATED APPEALS AND INTERFERENCES

Appellants, their Assignee and their legal representatives are unaware of the existence of any related appeals and/or interferences that will directly affect, be directly affected by, or have a bearing on the decision in the pending appeal.

III. STATUS OF CLAIMS

Claims 1-30 are pending in the instant application on appeal.

Claims 1-30 stand twice rejected and are the subject of the instant appeal.

The complete text of claims 1-30, as pending, is attached hereto in Appendix VIII.

IV. STATUS OF AMENDMENTS

No amendments were filed in the present application subsequent to the Final Rejection dated November 21, 2006. There are no unentered amendments in the present application.

V. SUMMARY OF CLAIMED SUBJECT MATTER

The following summary describes one preferred embodiment of the present invention. The scope of the present invention is not limited to the specific configuration or elements shown in the figures and described below.

Independent claim 1 recites a method of screening cookie files in a client machine (20), wherein a cookie file includes a cookie file source (page 3, lines 2-4; page 5, lines 18-19 and 28-29; page 7, lines 24-26; a cookie file source is an attribute of a cookie file, and thus it is inherent that a cookie file includes a cookie file source). A request from a subscriber is received at a server to send a list of cookie file sources to the client machine (page 6, lines 1-4 and Fig. 1). The list of cookie file sources is then downloaded from the server to the client machine (page 6, lines 1-4 and Fig. 1). The downloaded list of cookie file sources is then used to detect cookie files received at the client machine from cookie file sources on the downloaded list by comparing the cookie file source of any received cookie file to the cookie file sources on the downloaded

list (page 8, lines 15-17; page 9, lines 15-20; block 60 of Fig. 3).

Independent claim 7 recites a method of creating a composite list of cookie file sources in a client machine (page 5, lines 25-28; page 6, lines 8-14). A first exception list is created that includes the identity of cookie file sources that are permitted to store cookie files in the client machine (personal trustlist 16 shown in Figs. 1, 3, 5 and 6). A cookie file includes a cookie file source (page 3, lines 2-4; page 5, lines 18-19 and 28-29; page 7, lines 24-26; a cookie file source is an attribute of a cookie file, and thus it is inherent that a cookie file includes a cookie file source). A second exception list is created that includes the identity of cookie file sources that are not permitted to store cookie files in the client machine (personal blacklist 18 shown in Figs. 1, 3, 5 and 6). A master list of cookie file sources is received at the client machine from a service provider (page 6, lines 1-4). The master list is then modified in accordance with the first and second exception lists, wherein the composite list is the modified master list (page 5, lines 25-28; page 6, lines 8-14).

Independent claim 12 recites another method of creating a composite list of cookie file sources in a client machine (page 5, lines 25-28; page 6, lines 8-14). A master list of cookie file sources is received at the client machine from a service provider (page 6, lines 1-4). Cookie file sources from the master list that correspond to one or more trusted cookie file sources listed in the client machine are deleted (page 5, lines 25-28; page 6, lines 8-14). Cookie file sources are added to the master list that correspond to one or more untrusted cookie file sources listed in the client machine (page 5, lines 25-28; page 6, lines 8-14). The composite list is the master list as modified by any additions and deletions of trusted and untrusted cookie file sources (page 5, lines 25-28; page 6, lines 8-14).

Independent claims 16, 22 and 27 recite article of manufacture versions of claims 1, 7 and 12, respectively. Support for the article of manufacture limitation is provided on page 10, lines 20-24.

Independent claim 16 recites an article of manufacture (page 10, lines 20-24) for screening cookie files in a client machine (20), wherein a cookie file includes a cookie file source (page 3, lines 2-4; page 5, lines 18-19 and 28-29; page 7, lines 24-26; a cookie file source is an attribute of a cookie file, and thus it is inherent that a cookie file includes a cookie file source). A request from a subscriber is received at a server to send a list of cookie file sources to the client machine (page 6, lines 1-4 and Fig. 1). The list of cookie file sources is then

downloaded from the server to the client machine (page 6, lines 1-4 and Fig. 1). The downloaded list of cookie file sources is then used to detect cookie files received at the client machine from cookie file sources on the downloaded list by comparing the cookie file source of any received cookie file to the cookie file sources on the downloaded list (page 8, lines 15-17; page 9, lines 15-20; block 60 of Fig. 3).

Independent claim 22 recites an article of manufacture (page 10, lines 20-24) for creating a composite list of cookie file sources in a client machine (page 5, lines 25-28; page 6, lines 8-14). A first exception list is created that includes the identity of cookie file sources that are permitted to store cookie files in the client machine (personal trustlist 16 shown in Figs. 1, 3, 5 and 6). A cookie file includes a cookie file source (page 3, lines 2-4; page 5, lines 18-19 and 28-29; page 7, lines 24-26; a cookie file source is an attribute of a cookie file, and thus it is inherent that a cookie file includes a cookie file source). A second exception list is created that includes the identity of cookie file sources that are not permitted to store cookie files in the client machine (personal blacklist 18 shown in Figs. 1, 3, 5 and 6). A master list of cookie file sources is received at the client machine from a service provider (page 6, lines 1-4). The master list is then modified in accordance with the first and second exception lists, wherein the composite list is the modified master list (page 5, lines 25-28; page 6, lines 8-14).

Independent claim 27 recites another article of manufacture (page 10, lines 20-24) for creating a composite list of cookie file sources in a client machine (page 5, lines 25-28; page 6, lines 8-14). A master list of cookie file sources is received at the client machine from a service provider (page 6, lines 1-4). Cookie file sources from the master list that correspond to one or more trusted cookie file sources listed in the client machine are deleted (page 5, lines 25-28; page 6, lines 8-14). Cookie file sources are added to the master list that correspond to one or more untrusted cookie file sources listed in the client machine (page 5, lines 25-28; page 6, lines 8-14). The composite list is the master list as modified by any additions and deletions of trusted and untrusted cookie file sources (page 5, lines 25-28; page 6, lines 8-14).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

PART 1: Claims 1, 2, 4-8, 10-17, 19-23 and 25-30 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Walker et al. (hereafter, "Walker") in view of Shrader.

PART 2: Claims 3, 9, 18 and 24 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Walker in view of Shrader and Julien Jay (Norton Internet Security 2000 (NIS 2000)).

VIID. ARGUMENTS – REJECTIONS UNDER 35 U.S.C. § 103

PART 1. Claims 1, 2, 4-8, 10-17, 19-23 and 25-30 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Walker in view of Shrader.

A. There is a clear error in the Examiner's Final Rejection of claims 1, 7, 12, 16, 22 and 27 because Walker in view of Shrader do not disclose or suggest any of steps (a)-(c) of claims 1 and 16, at least step (c) of claims 7 and 22, and at least step (a) of claims 12 and 27

i. Background to Applicants' Invention

The following text portion from page 2, lines 19-30 of the present specification highlights one of the deficiencies in the prior art that the presently claimed invention addresses:

> There are software programs that let users create a profile of which types of cookie files they will accept. However, there is no guarantee that cookie files generated by companies with a history of abusing the use of cookie files will be screened out, nor is there a universal reference source for determining which cookie file sources should not be accepted. What is needed is a professional service that constantly researches and evaluates cookie file sources (e.g., websites), cookie files, consumer complaints and other statistical data, and develops and electronically distributes to subscribing computer users, on a periodic basis, a list of those cookie file sources that the service recommends should not be permitted to store cookie files in the subscribing user's computer. What is also needed is a user-friendly interface for enabling a user to easily and automatically modify the distributed list once it is received by the user's computer, such that the user may customize the list to meet his or her individual or organizational requirements.

Claims 1 and 16 are directed to the broad process for screening cookie files in a client machine by using a list of cookie file sources that is maintained by a server (e.g., the professional service referred to above that maintains a universal reference source) and downloaded to the client machine. Claims 7, 12, 22 and 27 are directed to a process for user editing of the list. Neither of the applied references disclose or suggest either of these claimed processes.

ii. Walker

Walker discloses a browser that is capable of accessing only web pages previously authorized by a parent or supervisor of a user of the browser. In a supervisor mode of operation, a parent can browse through any accessible web site and continually add approved web sites to a database of authorized web sites. Later, in a user mode of operation, the child is capable of accessing only those web sites that have been added to the authorized web site database. As described on column 11, lines 25-36 of Walker, the database of authorized web sites may be pre-populated with an initial pre-approved list of child-appropriate URL's that are downloaded from a remote server. The parent can then manually add more web sites to the list.

Numerous other previously applied references disclose downloading lists of child-safe websites. See, for example, the Norton Internet Security 2000 ("NIS 2000") Black web site list discussed on page 3 of the Response filed April 11, 2006 (mail date of April 6, 2006). As previously argued, this is not Applicants' invention because a list of web sites is not a list of cookie file sources. In fact, a list of web sites might not include any cookie file sources. Furthermore, the purpose of downloading a list of web sites is different than the purpose of downloading a list of cookie file sources. The purpose of downloading a list of web sites, as described in Walker or NIS 2000 is to allow users to block access to such sites. The purpose of downloading a list of cookie file sources, in one preferred embodiment of the present invention, is to prevent certain cookie files from becoming stored on a user machine, or to delete such cookie files if they were previously stored. Access to the website associated with the cookie file is not necessarily blocked.

On pages 2-3 of the outstanding rejection, the Examiner states that Walker discloses a client machine that requests a "list of sources" and a server that downloads a "list of sources" to the client machine. Throughout the entire prosecution history of this patent application, which has included eight Office Actions and a myriad of different prior art rejections, no prior art

reference has been cited that discloses or suggests any of steps (a)-(c) of claims 1 and 16, step (c) of claims 7 and 22, or step (a) of claims 12 and 27. On page 3 of the outstanding rejection, the Examiner admits that Walker does not disclose downloading a list of cookie file sources and relies instead upon Shrader for this limitation. However, as discussed below, Shrader also does not disclose downloading a list of cookie file sources, or steps (a)-(c) of claims 1 and 16, step (c) of claims 7 and 22, or step (a) of claims 12 and 27. Shrader thus fails to make up for the deficiencies in Walker and its equivalent prior art references.

iii. Shrader

Shrader discloses an improved cookie control process. Column 1, line 33 through column 2, line 19 of Shrader describes the problem in the art that is addressed, and reads as follows:

> A web browser automatically stores certain user data during the process of the user browsing the Internet...
>
> Another type of user data is a so-called "cookie." Because HTTP is a stateless protocol, a cookie can be set by a server to customize data to a particular user's web browser. Cookies thus provide a degree of "state" to HTTP. By default, a browser automatically stores cookie data without giving the user the option or knowledge of it being done. When a cookie is set as part of a HTTP transaction, it will include the path the cookie is valid for, the cookie's name and value, and other optional attributes, such as the expiration date for the cookie. In the prior art, a user can configure his or her web browser to show the cookie that the web server is attempting to set in a dialog box along with the options to set or cancel the cookie. After this initial display, the cookie value is unavailable for viewing or modification by the user. The browser may store cookie values in a text file, but this file can only be viewed outside of the browser and may only be updated when the browser is closed.
>
> Thus, like basic authentication data, cookie data typically is not exposed to the user. Thus, for example, after a user has agreed to accept cookies, there is no easy way for the user to modify the cookie without first bringing down the browser.
>
> It would be highly desirable to provide a web browser user with more control over what authentication and cookie data is stored on his or her behalf by a web browser or any other HTTP client application. The present invention addresses this problem.

Shrader provides a "cookie data display routine" to address this problem, as summarized on column 2, lines 48-67, which reads as follows (underlining added for emphasis):

> The cookie display routine displays cookie data that is sent to the web browser from a given web server. The display routine places a cookie icon as part of the text and icons that remain visible above the web browser frame. The web browser displays a no-cookie icon if no cookies are set for the path. When the user selects the cookie icon, the browser displays a dialog box showing all the stored cookie values for the URL or path. A display in the dialog box shows the attributes of each cookie and scroll bars may be used to let the user browse all the values. Buttons at the bottom of the dialog box allow the user to delete or modify an existing cookie value. If desired, the cookie display routine could allow additional cookie values to be set. In addition, the cookie display routine could allow the user to view, edit, or delete all cookie values, not just ones for the current URL.
>
> The cookie data display routine also enables a user to block all cookies from a particular site, such as a web server that returns nothing but advertisement graphics to subscribing URLs.

Shrader's cookie data display routine is initiated only when a user (client machine) attempts to retrieve a specific URL via a web browser. That is, Shrader's routine is initiated during a normal web surfing session and not as part of a process for downloading a list of cookie file sources in response to a request from a subscriber to send a list of cookie file sources (steps (a) and (b) of claims 1 and 16), or receiving at a client machine a master list of cookie file sources from a service provider (step (c) of claims 7 and 22; step (a) of claims 12 and 27). While Shrader arguably discloses "cookie file source(s)" in column 2, lines 64-67 as underlined above, this reference to cookie file sources has nothing whatsoever to do with a process for downloading a list of cookie file sources in response to a request from a subscriber to send a list of cookie file sources (steps (a) and (b) of claims 1 and 16), or receiving a master list of cookie file sources from a service provider (step (c) of claims 7 and 22; step (a) of claims 12 and 27). Accordingly, one cannot simply swap out Walker's downloaded list of URL's for Shrader's cookie file sources as asserted in the outstanding rejection because Shrader's cookie file sources are not downloaded in the same manner or for the same purpose as Walker's list of URL's.

In the outstanding Office Action, the Examiner refers to PATH 118 in CookieData Table 110 in Fig. 2 of Shrader as allegedly disclosing a "list of cookie file sources." The Examiner supports this contention by referring to column 5, lines 35-45 and column 1, lines 20-25 of Schrader. These portions of Shrader merely confirm Appellants' previous arguments that Schrader fails to make up for the noted deficiencies in Walker, namely, downloading a list of cookie file sources. Nowhere does Shrader disclose or suggest that the data residing in CookieData Table 110 is obtained from a downloaded list. Column 5, lines 35-45 of Schrader reads as follows (underlining added for emphasis):

> FIG. 2 shows representative data structures used in this invention. These structures are maintained in system or other memory (e.g., a hard disk). A BasicAuth Table 100 stores entries related to HTTP basic authentication. Each entry contains a number of data columns, including the server or domain name 102, userid 104 and password 106 that should be sent to the server. The realm name and other attributes may be included as well. A CookieData Table 110 stores entries related to cookies stored by the web browser on behalf of given web servers. Each entry contains a number of data columns, including the name 112 and value 114 of the cookie, the date that the cookie expires 116, and the path 118 and domain 120 for which the cookie is valid. Each entry also includes a secure flag 122, indicating if the cookie should be sent as part of a secure transaction, and a blocked flag 124, indicating if the cookie should be sent by the browser to the matching domain and path.

Shrader's cookie data display routine is initiated only when a user (client machine) attempts to retrieve a specific URL via a web browser. That is, Shrader's routine is initiated during a normal web surfing session and not as part of a process for downloading a list of cookie file sources in response to a request from a subscriber to send a list of cookie file sources (steps (a) and (b) of claims 1 and 16), or receiving at a client machine a master list of cookie file sources from a service provider (step (c) of claims 7 and 22; step (a) of claims 12 and 27). Again, one cannot simply swap out Walker's downloaded list of URL's for Shrader's cookie file sources as asserted in the outstanding rejection because Shrader's cookie file sources are not downloaded in the same manner or for the same purpose as Walker's list of URL's.

The Examiner's argument can be summarized as follows:

1. Walker discloses downloading a list of sources (e.g., web site URL addresses) to a client machine.

2. Schrader discloses storing a list of cookie file sources at a client machine. (As Appellants discussed above, this list is not downloaded to the client machine, nor is it received from a service provider.)

3. Therefore, it would have been obvious to download a list of cookie file sources to a client machine, or receive at a client machine a master list of cookie file sources from a service provider.

While the Examiner's logic has a simple appeal, it is a textbook example of improper hindsight recreation of Appellants' claimed invention. Shrader's scheme fails to address one of the purposes of Appellants' claimed invention, namely, to screen cookie files in a client machine by using a list of cookie file sources that is maintained by a server and downloaded to the client machine (claims 1 and 16), and to allow for user editing of the list (claims 7, 12, 22 and 27). Schrader's scheme requires the user to be responsible for cookie management by making all of the decisions regarding which cookie files should be blocked and which cookie files should be allowed. For example, in step 407 of Fig. 7 in Shrader, if a user tags a cookie to be blocked, the browser will not send the cookie back to the web site, thereby disrupting the process that the cookie is meant to control. One of the purposes of the claimed invention is to allow a service provider to provide the bulk of cookie management with the user optionally assisting in the process via a personal trustlist and personal blacklist. Shrader does not disclose or suggest any such arrangement. Instead, Shrader puts the burden of cookie management on users, most of whom have no sophisticated knowledge base to draw upon for making sound decisions regarding cookie management.

On page 3, last paragraph of the outstanding Office Action, the Examiner attempts to provide a reason for modifying Walker. However, the Examiner's reasoning is based on an incorrect premise that Shrader discloses a "downloaded list of web site URL addresses" (see last line of page 3). In fact, there is no downloading of any lists in Shrader, and none of the text portions referred to by the Examiner disclose or suggest any such downloading. The remaining explanations provided by the Examiner are thus equally flawed because they are based on a faulty premise.

On page 9 of the outstanding Office Action, the Examiner asserts that "features upon which applicant relies are not recited in the rejected claims(s)." Appellants respectfully traverse this assertion. Previous Appeal Briefs and the present Appeal Brief painstakingly identify exactly what limitations are not disclosed or suggested by any of the applied references. No limitations are being read into the claims to support Appellants' arguments regarding the deficiency of the applied references.

On page 13, first full paragraph of the outstanding Office Action, the Examiner mischaracterizes Appellants' invention. Specifically, the Examiner explains what he believes to be the "essence" of Appellant's invention. Appellants strongly object to such a characterization. Appellants have claimed a specific combination of steps that are believed to be novel and unobvious.

Furthermore, the essence of the invention as understood by the Examiner does not even properly capture the claimed invention. The Examiner states that the essence of the invention is to "detect a web site received at a client machine and then decide whether the received web site is on the list of downloaded...web sites." This is not Appellants' invention. In fact, this functionality is described in Walker and is also provided by many other software products that block browsers from displaying sites that are inappropriate for children. However, the Examiner correctly deemed Walker to be deficient in meeting all of the claim limitations. The essence of the invention thus inherently cannot meet the Examiner's characterization, otherwise the claims could be rejected as being anticipated by Walker.

On pages 14-15 of the outstanding Office Action, the Examiner provides text excerpts from Shrader, most of which were discussed above. None of these text excerpts provide the features that are discussed above as being absent from Walker.

iv. Walker in view of Shrader

Appellants do not dispute that Walker and Schrader are in the same art area or that there are compatibilities between them. However, all that the combination of Walker and Schrader would provide is a web site blocking tool that would also allow a user to provide enhanced cookie control for the web sites that are not blocked by Walker's process. Such a combination, however, would still not disclose or suggest the claimed invention.

B. Summary of claim limitations in claims 1, 7, 12, 16, 22 and 27 that are not disclosed or suggested by Walker in view of Shrader

For at least the reasons discussed above, none of the references applied against the independent claims disclose or suggest at least the following underlined limitations:

1. A method of screening cookie files in a client machine, wherein a cookie file includes a cookie file source, the method comprising:
(a) receiving, at a server, a request from a subscriber to send a list of cookie file sources to the client machine;
(b) downloading the list of cookie file sources from the server to the client machine; and
(c) using the downloaded list of cookie file sources to detect cookie files received at the client machine from cookie file sources on the downloaded list by comparing the cookie file source of any received cookie file to the cookie file sources on the downloaded list.

7. A method of creating a composite list of cookie file sources in a client machine, the method comprising:
(a) creating a first exception list including the identity of cookie file sources that are permitted to store cookie files in the client machine, wherein a cookie file includes a cookie file source;
(b) creating a second exception list including the identity of cookie file sources that are not permitted to store cookie files in the client machine;
(c) receiving at the client machine, from a service provider, a master list of cookie file sources; and
(d) modifying the master list in accordance with the first and second exception lists, wherein the composite list is the modified master list.

12. A method of creating a composite list of cookie file sources in a client machine, the method comprising:
(a) receiving at the client machine, from a service provider, a master list of cookie file sources;
(b) deleting cookie file sources from the master list that correspond to one or more trusted cookie file sources listed in the client machine; and
(c) adding cookie file sources to the master list that correspond to one or more untrusted cookie file sources listed in the client machine, wherein the composite list is the master list as modified by any additions and deletions of trusted and untrusted cookie file sources.

16. An article of manufacture for screening cookie files in a client machine, wherein a cookie file includes a cookie file source, the article of manufacture comprising a computer-readable medium holding computer-executable instructions for performing a method comprising:
(a) receiving, at a server, a request from a subscriber to send a list of

cookie file sources to the client machine;
(b) downloading the list of cookie file sources from the server to the client machine; and
(c) using the downloaded list of cookie file sources to detect cookie files received at the client machine from sources on the downloaded list by comparing the cookie file source of any received cookie file to the cookie file sources on the downloaded list.

22. An article of manufacture for creating a composite list of cookie file sources in a client machine, the article of manufacture comprising a computer-readable medium holding computer-executable instructions for performing a method comprising:
(a) creating a first exception list including the identity of cookie file sources that are permitted to store cookie files in the client machine, wherein a cookie file includes a cookie file source;
(b) creating a second exception list including the identity of cookie file sources that are not permitted to store cookie files in the client machine;
(c) receiving at the client machine, from a service provider, a master list of cookie file sources; and
(d) modifying the master list in accordance with the first and second exception lists, wherein the composite list is the modified master list.

27. An article of manufacture for creating a composite list of cookie file sources in a client machine, the article of manufacture comprising a computer-readable medium holding computer-executable instructions for performing a method comprising:
(a) receiving at the client machine, from a service provider, a master list of cookie file sources;
(b) deleting cookie file sources from the master list that correspond to one or more trusted cookie file sources listed in the client machine; and
(c) adding cookie file sources to the master list that correspond to one or more untrusted cookie file sources listed in the client machine, wherein the composite list is the master list as modified by any additions and deletions of trusted and untrusted cookie file sources.

Furthermore, the unique combination of steps (a)-(c) in claims 1 and 16; steps (a)-(d) in claims 7 and 22; and steps (a)-(c) in claims 12 and 27 are not disclosed or suggested by the applied references.

In view of the above remarks, claims 1, 7, 12, 16, 22 and 27 are believed to be patentable over Walker in view of Shrader.

C. Patentability of dependent claims 2, 4-6, 8, 10-11, 13-15, 17, 19-21, 23, 25-26 over Walker in view of Shrader

These dependent claims are believed to be patentable over the applied references for at least the reason that they are dependent upon allowable base claims and because they recite additional patentable elements and steps.

PART 2. Claims 3, 9, 18 and 24 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Walker in view of Shrader and NIS 2000.

These dependent claims are also believed to be patentable over the applied references for at least the reason that they are dependent upon allowable base claims and because they recite additional patentable elements and steps. Furthermore, NIS 2000 does not make up for any of the above-highlighted deficiencies in Walker or Schrader.

PART 3. The claims are not obvious in view of KSR International Co. v. Teleflex, Inc.

In *KSR Int'l v. Teleflex Inc.*, 127 S. Ct. 1727 (2007), hereafter, "KSR", the Supreme Court stated that the motivation/suggestion/teaching test is merely one test that can be applied to an obviousness inquiry. For the reasons discussed above, the Examiner's rejection clearly fails this test. Furthermore, none of the other tests sanctioned by the Supreme Court in KSR for determining obviousness are relevant to this case, and the Examiner has not set forth any facts or evidence to support any of the other tests.

First, KSR is not even relevant to this situation because even if Walker was modified with features present in Shrader based on "obvious to try" reasoning, the modified version of Walker would still be missing claim features. As discussed above, all that the combination of Walker and Schrader would provide is a web site blocking tool that would also allow a user to provide enhanced cookie control for the web sites that are not blocked by Walker's process. Such a combination, however, would still not disclose or suggest the above-highlighted claim features.

Second, even if the Examiner's rejection is based on the obviousness of modifying Walker based on Schrader, or is based on the combination of these references, the Examiner has still failed to identify the reason that would have prompted a person of ordinary skill in the art to combine the prior art elements so as to achieve the claimed invention. The closest that the

Examiner has come to providing any reasons for modifying Walker is discussed in the paragraph spanning pages 3-4 of the outstanding Office Action. Two reasons appear to be provided. The first reason reads as follows:

> It would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify Walker to include a list of cookie file sources as taught by Shrader for the purpose of reviewing the cookie files received at the client's machine for the purpose of controlling cookies planted/stored on a client's machine by a web site [Shrader: col 2, lines 60-63, the cookie display routine could allow the user to view, edit or delete cookie values]. (page 13, line 18 through page 14, line 3 of the Examiner's Answer)

This reason is precisely the kind of reason that constitutes impermissible hindsight recreation of Appellants' invention. Shrader's cookie display routine is a manual process performed by a user and does not use a downloaded list of cookie file sources. That is not Appellants' claimed invention. To build Appellants' invention, the Examiner has impermissibly altered the manner of operation of Shrader so that the contents of the Shrader's CookieData Table 110 is now obtained from a downloaded list. Presumably, this would occur by modifying Walker to download a list of cookie file sources, instead of its intended manner of operation which is to download a list of URL's. Again, this modification would destroy the intended manner of operation of Walker, which is to allow a browser to access only web pages previously authorized by a parent or supervisor of the user (see line 1 of Walker's Abstract). Walker has nothing whatsoever to do with cookies, or cookie control, and does not even mention cookies anywhere in its disclosure.

The second reason reads as follows (underlining added for emphasis):

> Furthermore, Schrader discloses using the downloaded list of web site URL addresses to detect a cookie file received at the user's machine by comparing the URL address of the received cookie file with at least one URL address on the downloaded list of web site URL addresses [col 2, lines 64-67, block all cookies from a particular site] (page 14, lines 3-7 of Examiner's Answer)

This reason is based on an incorrect premise that Shrader discloses a "downloaded list of web site URL addresses," as also discussed above. In fact, there is no downloading of any lists in

Shrader, and none of the text portions referred to by the Examiner disclose or suggest any such downloading.

Third, the Examiner's proposed modification to Walker to provide a list of cookie file sources fails the new "obvious to try" test sanctioned by KSR. According to KSR,

> "When there is a design need or market pressure to solve a problem and there are a finite number of identified, predictable solutions, a person of ordinary skill has good reason to pursue the known options within his or her technical grasp. If this leads to the anticipated success, it is likely the product not of innovation but of ordinary skill and common sense. In that instance the fact that a combination was obvious to try might show that it was obvious under §103." (emphasis added).

Thus, the fact that something was "obvious to try" might be sufficient to prove obviousness when:

i. a design need or market pressure to solve a problem existed; and

ii. there was a finite number of identified predictable solutions; and

iii. the success anticipated by trying such solutions was realized.

Here, the Examiner has failed to identify the existence of any design need or market pressure to solve a problem. The Examiner has not pointed out any reference or industry source that discusses the complexity of managing cookie files using existing tools, or the desire or market pressure to provide better tools. It is only in hindsight, after Appellants have described an improved way of managing cookie files, that the claimed invention is deemed obvious. Stated simply, the Examiner's proposed modification to Shrader is a textbook example of improper hindsight modification of a prior art reference to build Appellants' invention.

Accordingly, none of the Examiner's reasons pass muster under a KSR analysis.

PART 4. Conclusion

For the reasons set forth above, Appellants respectfully submit that pending claims 1-30 are patentable over the prior art applied by the Examiner. Reversal of the rejections and issuance of a Notice of Allowance are respectfully requested at the earliest opportunity.

VIII. APPENDIX OF CLAIMS

1. A method of screening cookie files in a client machine, wherein a cookie file includes a cookie file source, the method comprising:

(a) receiving, at a server, a request from a subscriber to send a list of cookie file sources to the client machine;

(b) downloading the list of cookie file sources from the server to the client machine; and

(c) using the downloaded list of cookie file sources to detect cookie files received at the client machine from cookie file sources on the downloaded list by comparing the cookie file source of any received cookie file to the cookie file sources on the downloaded list.

2. The method of claim 1, further comprising:

(d) creating a first exception list including the identity of cookie file sources that are permitted to store cookie files in the client machine;

(e) creating a second exception list including the identity of cookie file sources that are not permitted to store cookie files in the client machine; and

(f) modifying the downloaded list in accordance with the first and second exception lists.

3. The method of claim 1, further comprising:

(d) receiving updates of the downloaded list from the server on a periodic basis.

4. The method of claim 1, further comprising:

(d) displaying a message at the client machine indicating that a cookie file received from a cookie file source on the downloaded list has been detected.

5. The method of claim 1, further comprising:

(d) removing detected cookie files stored in the client machine.

6. The method of claim 1, further comprising:

(d) preventing detected cookie files from being stored in the client machine.

7. A method of creating a composite list of cookie file sources in a client machine, the method comprising:

(a) creating a first exception list including the identity of cookie file sources that are permitted to store cookie files in the client machine, wherein a cookie file includes a cookie file source;

(b) creating a second exception list including the identity of cookie file sources that are not permitted to store cookie files in the client machine;

(c) receiving at the client machine, from a service provider, a master list of cookie file sources; and

(d) modifying the master list in accordance with the first and second exception lists, wherein the composite list is the modified master list.

8. The method of claim 7, wherein the composite list is stored in the client machine independent of the first exception list, the second exception list and the received master list.

9. The method of claim 7, further comprising:

(e) receiving updates of the master list from the service provider on a periodic basis.

10. The method of claim 7, further comprising:

(e) removing stored cookie files received at the client machine from cookie file sources on the composite list by comparing the cookie file source of stored cookie files to the cookie file sources on the composite list, and removing any stored cookie files that have matching cookie file sources.

11. The method of claim 7, further comprising:

(e) preventing cookie files received at the client machine from cookie file sources on the composite list from being stored in the client machine by comparing the cookie file source of received cookie files to the cookie file sources on the composite list and, preventing storage of any received cookie files that have matching cookie file sources.

12. A method of creating a composite list of cookie file sources in a client machine, the method comprising:

(a) receiving at the client machine, from a service provider, a master list of cookie file sources;

(b) deleting cookie file sources from the master list that correspond to one or more trusted cookie file sources listed in the client machine; and

(c) adding cookie file sources to the master list that correspond to one or more untrusted cookie file sources listed in the client machine, wherein the composite list is the master list as modified by any additions and deletions of trusted and untrusted cookie file sources.

13. The method of claim 12, wherein the master list and the composite list are stored

independently in the client machine.

14. The method of claim 12, further comprising:

(d) removing cookie files stored in the client machine and received from cookie file sources on the composite list by comparing the cookie file source of stored cookie files to the cookie file sources on the composite list, and removing any stored cookie files that have matching cookie file sources, wherein a cookie file includes a cookie file source.

15. The method of claim 12, further comprising:

(d) preventing cookie files received at the client machine from sources on the composite list from being stored in the client machine by comparing the cookie file source of received cookie files to the cookie file sources on the composite list, and preventing storage of any received cookie files that have matching cookie file sources, wherein a cookie file includes a cookie file source.

16. An article of manufacture for screening cookie files in a client machine, wherein a cookie file includes a cookie file source, the article of manufacture comprising a computer-readable medium holding computer-executable instructions for performing a method comprising:

(a) receiving, at a server, a request from a subscriber to send a list of cookie file sources to the client machine;

(b) downloading the list of cookie file sources from the server to the client machine; and

(c) using the downloaded list of cookie file sources to detect cookie files received at the client machine from sources on the downloaded list by comparing the cookie file source of any received cookie file to the cookie file sources on the downloaded list.

17. The article of manufacture of claim 16, wherein the computer-executable instructions perform a method further comprising:

(d) creating a first exception list including the identity of cookie file sources that are permitted to store cookie files in the client machine;

(e) creating a second exception list including the identity of cookie file sources that are not permitted to store cookie files in the client machine; and

(f) modifying the downloaded list in accordance with the first and second exception lists.

18. The article of manufacture of claim 16, wherein the computer-executable instructions perform a method further comprising:

(d) receiving updates of the downloaded list from the server on a periodic basis.

19. The article of manufacture of claim 16, wherein the computer-executable instructions perform a method further comprising:

(d) displaying a message at the client machine indicating that a cookie file received from a cookie file source on the downloaded list has been detected.

20. The article of manufacture of claim 16, wherein the computer-executable instructions perform a method further comprising:

(d) removing detected cookie files stored in the client machine.

21. The article of manufacture of claim 16, wherein the computer-executable instructions

perform a method further comprising:

(d) preventing detected cookie files from being stored in the client machine.

22. An article of manufacture for creating a composite list of cookie file sources in a client machine, the article of manufacture comprising a computer-readable medium holding computer-executable instructions for performing a method comprising:

(a) creating a first exception list including the identity of cookie file sources that are permitted to store cookie files in the client machine, wherein a cookie file includes a cookie file source;

(b) creating a second exception list including the identity of cookie file sources that are not permitted to store cookie files in the client machine;

(c) receiving at the client machine, from a service provider, a master list of cookie file sources; and

(d) modifying the master list in accordance with the first and second exception lists, wherein the composite list is the modified master list.

23. The article of manufacture of claim 22, wherein the composite list is stored in client machine independent of the first exception list, the second exception list and the received master list.

24. The article of manufacture of claim 22, wherein the computer-executable instructions perform a method further comprising:

(e) receiving updates of the master list from the service provider on a periodic basis.

25. The article of manufacture of claim 22, wherein the computer-executable instructions

perform a method further comprising:

(e) removing stored cookie files received at the client machine from cookie file sources on the composite list by comparing the cookie file source of stored cookie files to the cookie file sources on the composite list, and removing any stored cookie files that have matching cookie file sources.

26. The article of manufacture of claim 22, wherein the computer-executable instructions perform a method further comprising:

(e) preventing cookie files received at the client machine from cookie file sources on the composite list from being stored in the client machine by comparing the cookie file source of received cookie files to the cookie file sources on the composite list and, preventing storage of any received cookie files that have matching cookie file sources.

27. An article of manufacture for creating a composite list of cookie file sources in a client machine, the article of manufacture comprising a computer-readable medium holding computer-executable instructions for performing a method comprising:

(a) receiving at the client machine, from a service provider, a master list of cookie file sources;

(b) deleting cookie file sources from the master list that correspond to one or more trusted cookie file sources listed in the client machine; and

(c) adding cookie file sources to the master list that correspond to one or more untrusted cookie file sources listed in the client machine, wherein the composite list is the master list as modified by any additions and deletions of trusted and untrusted cookie file sources.

28. The article of manufacture of claim 27, wherein the master list and the composite list are stored independently in the client machine.

29. The article of manufacture of claim 27, wherein the computer-executable instructions perform a method further comprising:

(d) removing cookie files stored in the client machine and received from cookie file sources on the composite list by comparing the cookie file source of stored cookie files to the cookie file sources on the composite list, and removing any stored cookie files that have matching cookie file sources, wherein a cookie file includes a cookie file source.

30. The article of manufacture of claim 27, wherein the computer-executable instructions perform a method further comprising:

(d) preventing cookie files received at the client machine from sources on the composite list from being stored in the client machine by comparing the cookie file source of received cookie files to the cookie file sources on the composite list, and preventing storage of any received cookie files that have matching cookie file sources, wherein a cookie file includes a cookie file source.

IX. APPENDIX OF EVIDENCE

A copy of a § 1.131 Declaration filed April 6, 2007 (entered on April 11, 2006) is attached as Evidence Appendix A and a copy of a 1.131 Declaration filed November 9, 2006 is attached as Evidence Appendix B. These Declarations were submitted to overcome a rejection over Buck '912. These Declarations were considered by the Examiner in the Office Actions dated May 15, 2006 and November 21, 2006. As discussed above, in a telephone call on December 7, 2006, the Examiner clarified that the § 102(e) rejection over U.S. Patent Application Publication No. 2002/0055912 (Buck) was withdrawn in the November 21, 2006 Office Action.

Regarding 37 CFR § 41.37(c)(ix), these Declarations were not "relied upon by appellant in the appeal" because the Examiner withdrew the rejection over Buck. However, these Declarations are being provided because they were requested in the "Order Returning Undocketed Appeal to the Examiner" dated December 5, 2007.

JUN 23 2008
PATENT & TRADEMARK OFFICE

COPY – Evidence Appendix A

I HEREBY CERTIFY THAT THIS CORRESPONDENCE IS BEING DEPOSITED WITH THE UNITED STATES POSTAL SERVICE AS FIRST CLASS MAIL IN AN ENVELOPE ADDRESSED TO: COMMISSIONER FOR PATENTS, P.O. BOX 1450, ALEXANDRIA, VA 22313-1450, ON THE DATE INDICATED BELOW.

BY: Gladys E. Morales Date: April 4, 2006

MAIL STOP AMENDMENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re Patent Application of: Adam R. Schran et al.		
Conf. No.:	3079	Group Art Unit: 2161
Appln. No.:	09/820,054	Examiner: Etienne Pierre Leroux
Filing Date:	March 28, 2001	Attorney Docket No.: 10397-1U1
Title:	SYSTEM AND METHOD FOR NETWORK ADMINISTRATION AND LOCAL ADMINISTRATION OF PRIVACY PROTECTION CRITERIA	

DECLARATION OF PRIOR INVENTION TO OVERCOME CITED PATENT (37 CFR § 1.131)

PURPOSE OF DECLARATION

This declaration is being submitted to establish completion of the invention in this application in the United States at a date prior to October 20, 2000, which is the earliest possible effective date of the prior art U.S. Patent Application Publication No. 2002/0055912 (Buck), which was cited and applied by the Examiner in an Office Action dated November 18, 2005.

The persons making this declaration are the inventors, and are thus qualified to submit this declaration under 37 CFR § 1.131.

PE 1600
JN 2 3 2006
PAT & TRADEMARK OFFICE

FACTS AND DOCUMENTARY EVIDENCE

To establish the date of completion of the invention of this patent application, copies of the following documents and supporting statements are submitted as evidence:

Documents

EXHIBIT 1: Screen shot printout of a file folder that contains the executable code (.exe) of a beta version of ActivePrivacy.

EXHIBIT 2: Document entitled "INTELLECTUAL PROPERTY NEEDS ASSESSMENT" which provides an overview of the technical capabilities of ActivePrivacy.

EXHIBIT 3: Patentability search memorandum.

EXHIBIT 4: Email from a customer of ActivePrivacy.

EXHIBIT 5: Chart of independent claim limitations that shows documentation for each claim limitation.

Supporting statements

1. The blacked out dates labeled as D1-D4[1] in Exhibit 1 are all prior to October 20, 2000.

2. The blacked out date labeled D1 in Exhibit 2 is prior to October 20, 2000.

3. The blacked out dates labeled D1 and D2 in Exhibit 3 are both prior to October 20, 2000.

4. The blacked out dates labeled D1 and D2 in Exhibit 4 are both prior to October 20, 2000.

5. Each claim limitation in Exhibit 5 is supported by documentation that is dated prior to October 20, 2000. Text portions T1-T6 (there is no T2) referred to in Exhibit 5 correspond to respectively labeled text portions in Exhibits 2 and 3.

6. A beta version of ActivePrivacy was created and released prior to October 20, 2000, as evidenced by Exhibits 1 and 2. See, text portion T7 of Exhibit 2.

7. A commercial subscription-based version of ActivePrivacy was released and made available for a license fee prior to October 20, 2000, as evidenced by Exhibit 4.

[1] D4 refers only to the 272 kB ActivePrivacy.exe file.

A2

8. The beta and commercial version of ActivePrivacy both contained all of the functionality of the claim limitations shown in Exhibit 5. General descriptions of such functionality are given in Exhibits 2 and 3.

9. ActivePrivacy is the commercial name of a software product associated with the presently claimed invention, as further evidenced by Figs. 4 and 6 of the present invention which show screen shots labeled with "ActivePrivacy."

From the attached documents and the supporting statements, we submit that it has been established that the invention in this application was made prior to October 20, 2000, which is the earliest possible effective date.

TIME OF PRESENTATION OF THE DECLARATION

This declaration is submitted prior to final rejection.

DECLARATION

As a person signing below:

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

SIGNATURES

Full name of first or sole inventor: Adam R. Schran

Inventor's Signature: 

Date: 4/5/2006

Residence: Philadelphia, Pennsylvania

Citizenship: United States of America

Post Office Address: 217 Church St #4 Phila PA 19147

Full name of second joint inventor: Robert E. Darlington

Inventor's Signature

Date

Residence: Los Alamos, New Mexico

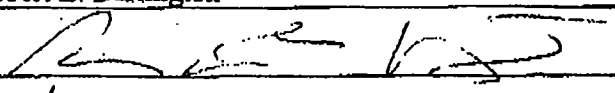
Citizenship: United States of America

Post Office Address: 3260-B Orange Street, Los Alamos, New Mexico 87544

A3B

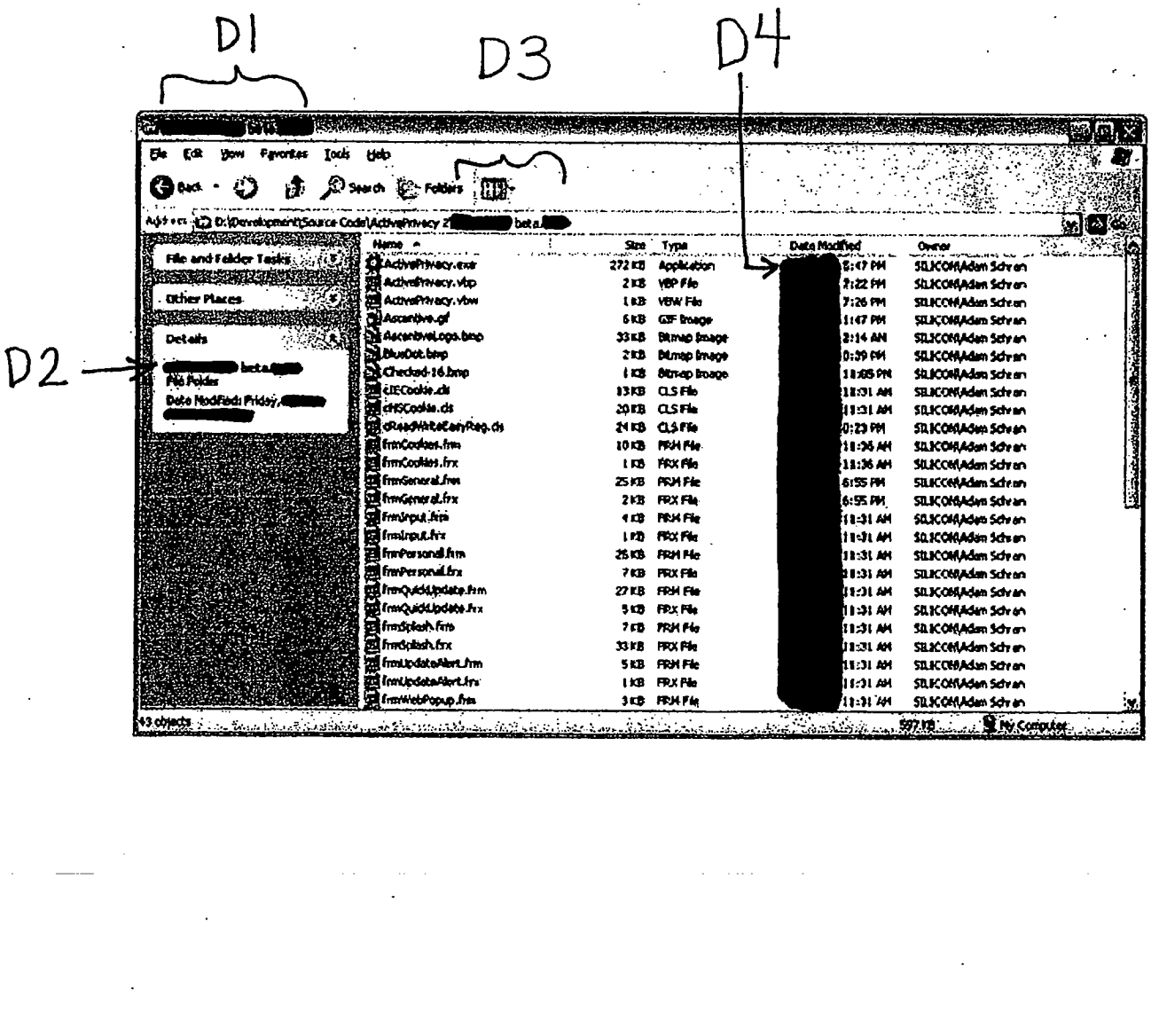
SIGNATURES

Full name of first or sole inventor	Adam R. Schran
Inventor's Signature	
Date	
Residence	Philadelphia, Pennsylvania
Citizenship	United States of America
Post Office Address	

Full name of second joint inventor	Robert E. Darlington
Inventor's Signature	
Date	4/6/06
Residence	Los Alamos, New Mexico
Citizenship	United States of America
Post Office Address	3260-B Orange Street, Los Alamos, New Mexico 87544

A4

EXHIBIT 1 of "Declaration of Prior Invention..."
(Application No. 09/820,054)



D1 { [redacted]

INTELLECTUAL PROPERTY NEEDS ASSESSMENT

Adam Schran

Ascentive

Introduction

Ascentive, an Internet software company, was founded in November 1998 on the proverbial 'back of the napkin' and launched in January 1999. Since then, revenue has grown at an average 50% per month, resulting from a successful focus on building a network of 3,000+ affiliate web sites to bootstrap the company.

Products

Since launch, Ascentive has brought to market two consumer software products for Windows:

- WebROCKET Internet Optimizer – An instant speed boost for any dial-up or high-speed Internet connection.
- WinROCKET Computer Optimizer – Performance booster for all computers running Windows 95 and 98.

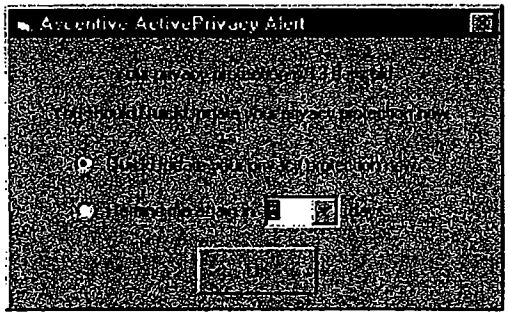
ActivePrivacy Overview T7

ActivePrivacy, currently undergoing beta testing, represents a leap forward in privacy protection from the current tools-driven convention to a service-driven model.

In the current schema, Internet users have one of three options:

- Head in the sand: Do nothing about potential privacy violations.
- Scorched earth: Disable all avenues for privacy violations, thus reducing the utility and automation of many web sites.
- Do it yourself: Scan for potential privacy violations yourself, consuming time and energy.

ActivePrivacy's service approach is superior to all three methods.



T1 {

- Customer subscribes to the ActivePrivacy QuickUpdate privacy service to manage their privacy needs. The QuickUpdate service includes the latest privacy protection, consisting of a "Watchlist" of sites that use cookie files to store unique or identifying information.

T3 {

- ActivePrivacy, the client software, scans for privacy violations and takes corrective action while you use the Internet. To trigger potential privacy violations, the Watchlist (retrieved by the client software from Ascentive's QuickUpdate server) is merged with the end user's Blacklist, exempting any sites in the end user's Trustlist.

T6 {

T4 T5

- The end user is reminded to keep their Watchlist up to date by QuickUpdating frequently.

Inventions

We believe the following innovations in ActivePrivacy are new and non-obvious, and are good candidates for patent protection.

- Determing and taking corrective action for privacy violations that have already occurred by merging "QuickUpdate" Watchlist privacy protection with the end-user's Blacklist and Trustlist.
- "Privacy safe browsing", a browser window in the client/server that uses the QuickUpdate privacy protection to preemptively strike against privacy violations.
- The ActivePrivacy QuickUpdate server, a system that distributes incremental updates to end users' privacy protection through the QuickUpdate client software.

E. BIT 3 of "Declaration of Prior Inve n..."
(Application No. 09/820,054)

AKIN, GUMP, STRAUSS, HAUER & FELD, L.L.P.

ATTORNEYS AT LAW
One Commerce Square - 2005 Market Street - Suite 2200
PHILADELPHIA, PA 19103-7086
Telephone: (215) 965-1200 - FAX: (215) 965-1210
E-MAIL: &@@akingump.com

CONFIDENTIAL D1→ [redacted] **CONFIDENTI**

VIA FACSIMILE: 703-415- 1017 - (Confirmation copy via First-Class Mail)

SEARCHER: Randy Lacasse **Client No.:**

210397.0001

FROM: Louis Sickles **PAGE 1 OF 4** **DEADLINE:**

D2→ [redacted]

( ) Telephone Confirmation (X) New Instructions ( ) Fax Confirmation

INSTRUCTIONS: ( ) Detailed Instructions Attac

Please conduct a patentability search on a regular basis for a Method of Expunging Unwanted Cookies from a Computer.

A "cookie" is a short piece of data which is transmitted from certain Internet hypertext transfer protocol (HTTP) server computers to a client computer when the HTTP server connects to the client computer in response to a uniform resource locator (URL) request from the client computer. The cookie includes, in part, data related to the web page accessed by the client computer and the domain attributes of the server. Cookies transmitted from individual server computers are separately stored in the memory of the client computer.

In subsequent transactions between the client computer and a server which had previously transmitted a cookie to the client computer, (or a server included in the domain specified by the server), a copy of the cookie stored in the client computer and linked to that domain address is automatically included in the client computer's URL request. In this way, the server receiving the URL request knows that the user has previously connected to the server and can (if desired) direct the client's access to a specific page (or pages) on its web site.

Cookies are typically used by Internet shopping sites to keep track of the user's shopping cart. When a user first visits an Internet shopping site, the user is sent a cookie containing the name (ID number) of a shopping cart. Each time an item is selected for purchase, the shopping site correlates that selection to the shopping cart by the shopping cart ID number

contained in the cookie and adds the selection to the cookie. When the user is done with shopping, the checkout page lists all of the items in the shopping cart tied to the cookie. Without cookies, the user would have to keep track of all the items that the user wanted to buy and type them into the checkout page at the conclusion of the transaction, or buy each item one at a time. Alternative to accumulating the shopping cart data in a single cookie, the shopping site could send a separate cookie containing the selected item number to the client computer whenever an item was selected to purchase.

One of the less admirable and controversial uses of cookies is for tracking the browsing and buying habits of individual web users. On a single web site or a group of web sites within a single sub-domain, cookies can be used to see what web pages the user visits and how often the user visits them. On web sites which display banner advertisements from a single marketing site, cookies can be used to track the browsing habits on all of the web sites being serviced by the marketing site. Tracking is accomplished by issuing a cookie with the marketing site's domain specified when the user clicks on the advertisement. Subsequent connection of a user to any web site displaying one of the marketing site's advertisements results in a cookie being sent to the marketing site. The marketing site can correlate the users buying habits from the plurality of cookies and develop a profile of the user.

Currently, a user has only two options if the user prefers not to have his web browsing habits tracked. Commercial browsers, (e.g.. Internet Explorer or Netscape Navigator), provide options that: (1) prevent any cookie from being stored in the user's computer, (2) notify the user each time a cookie is sent to the browser allowing the user to reject or accept the cookie, or (3) accept all cookies. None of the aforementioned options is entirely satisfactorily. In the first case, the user will be prevented from connecting with many desirable sites that do not abuse the use of the cookie. In the second case, the user will be likely be annoyed by the notification messages which may occur numerous times during a connection to a single web site.

Software applications are known which can be installed in a client computer to give the user additional control over cookies. These software packages typically allow the user to accept, reject or delete cookies from the client computer that originate from user specified web sites. However, all of these known software packages require the user to develop the list of unwanted web sites.

In the proposed system concept an HTTP server maintains a watch list of Internet sites that use cookies to store unique or identifying information about a user. The user's computer contains both a user developed black list of Internet sites for which the user prefers not to have cookies stored in his system, and a user developed list of trusted Internet sites for which the user has perfect trust. In use, the user is periodically prompted to connect the client computer with the HTTP server containing the watch list. In response, the HTTP server downloads the watch list to the user's computer. The watch list is combined with the user's blacklist and the user's trusted list to create a composite list of Internet sites. The composite list is formed by subtracting sites on the trusted list from the watch list and adding the result to the user's black list.

The user's software can operate in two different modes. In the first mode, the user's software deletes offending cookies from the user's memory based on the composite list. In this mode, the user may set the software to execute at any periodicity he chooses, from seconds to hours. In the second mode, the software operates continuously to intercept cookies as the cookies are received from the offending web server. The watch list may also include attributes that characterize the Internet sites using cookies based on the degree of identifying information contained in the cookie. In these instances, the user would be notified that the cookie was present in his system or is being sent to the system and the user would be given the option of editing the composite list to accept or reject cookies from that site.

Note that a similar concept is used to download anti-virus software to client computers. However, the concept of the present invention differs in at least two respects: (1) the combining of the watch list, the black list and the trusted list and (2) the concept of detecting and rejecting the cookie as it is received by the user's computer.

The following words and phrases are sometimes usd synnomynously for cookies and may assist in searching for references related to "cookies": persistent cookie; token; state object; and state management.

In summary, please focus your search on the following concepts: (1) a computer software program residing in a server computer that maintains a watch list of computer servers that use cookies to store unique or identifying information about a user and upon request downloads the watch list to a subscribing client computer; and (2) a computer program that resides in a subscribing client computer that maintains a black list and a trusted list and uses the

black list and the trusted list in conjunction with the downloaded watch list to either delete unwanted cookies from the client computer memory and/or reject unwanted cookies as they are received in the client computer.

If you require additional information please contact me at the above 215-965-1294.

Thank you.

FOR SEARCHER'S USE ONLY

Date Completed: _____
Time: _____
Costs: _____

EXHIBIT 4 of "Declaration of Prior Invention..."
(Application No. 09/820,054)

D1

CSNavy@aol.com, 01:53 AM [redacted], Active Privacy Problem

D2

From: CSNavy@aol.com
Date: Sat [redacted] 02:53:25 EDT
Subject: Active Privacy Problem
To: comments@ascentive.com
X-Mailer: AOL 5.0 for Windows sub 119

Dear Sir Or Madam:
After the first few days of using ActivePrivacy I've been unable to keep the program running on my computer. After 20 minutes to 1 hour a window pops up with Run error Division by zero and the program shuts down once this is acknowledged.
This makes the ActivePrivacy program virtually useless to me. Unless I can find a solution to this I will discontinue using it and uninstall this program.

V/R
Kelsey Baker

A11

EXHIBIT 5 of "Declaration of Prior Invention..."
(Application No. 09/820,054)

Chart of independent claim limitations that shows documentation for each claim limitation

Text of independent claims	Exhibit(s) that support claim limitations
1. A method of screening cookie files in a client machine, the method comprising:	
(a) receiving, at a server, a request from a subscriber to send a list of cookie file sources to the client machine;	Exhibit 2: T1 Exhibit 3: T1
(b) downloading the list from the server to the client machine; and	Exhibit 2: T1 Exhibit 3: T1
(c) using the downloaded list to detect cookie files received at the client machine from sources on the downloaded list.	Exhibit 2: T3 Exhibit 3: T3
16.	Same as claim 1

Text of independent claims	Exhibit(s) that support claim limitations
7. A method of creating a composite list of cookie file sources in a client machine, the method comprising:	
(a) creating a first exception list including the identity of sources that are permitted to store cookie files in the client machine;	Exhibit 2: T4 Exhibit 3: T4
(b) creating a second exception list including the identity of sources that are not permitted to store cookie files in the client machine;	Exhibit 2: T5 Exhibit 3: T5
(c) receiving at the client machine, from a service provider, a master list of cookie file sources; and	Exhibit 2: T1 Exhibit 3: T1
(d) modifying the master list in accordance with the first and second exception lists, wherein the composite list is the modified master list.	Exhibit 2: T6 Exhibit 3: T6
22.	Same as claim 7

Text of independent claims	Exhibit(s) that support claim limitations
12. A method of creating a composite list of cookie file sources in a client machine, the method comprising:	
(a) receiving at the client machine, from a service provider, a master list of cookie file sources;	Exhibit 2: T1 Exhibit 3: T1
(b) deleting cookie file sources from the master list that correspond to one or more trusted cookie file sources listed in the client machine; and	Exhibit 2: T4, T6 Exhibit 3: T4, T6
(c) adding cookie file sources to the master list that correspond to one or more untrusted cookie file sources listed in the client machine, wherein the composite list is the master list as modified by any additions and deletions of trusted and untrusted cookie file sources.	Exhibit 2: T5, T6 Exhibit 3: T5, T6
27.	Same as claim 12

A13

JUN 23 2008
PATENT & TRADEMARK OFFICE

COPY
Evidence Appendix B

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re Patent Application of: Adam R. Schran et al.		:	
Conf. No.:	3079	:	Group Art Unit: 2161
Appln. No.:	09/820,054	:	Examiner: Etienne Pierre Leroux
Filing Date:	March 28, 2001	:	Attorney Docket No.: 10397-1U1
Title:	SYSTEM AND METHOD FOR NETWORK ADMINISTRATION AND LOCAL ADMINISTRATION OF PRIVACY PROTECTION CRITERIA	:	

SUPPLEMENTAL DECLARATION OF PRIOR INVENTION TO OVERCOME CITED PATENT (37 CFR § 1.131)

PURPOSE OF DECLARATION

This supplemental declaration is being submitted to establish completion of the invention in this application in the United States at a date prior to October 20, 2000, which is the earliest possible effective date of the prior art U.S. Patent Application Publication No. 2002/0055912 (Buck), which was cited and applied by the Examiner in Office Actions dated November 18, 2005 and May 15, 2006.

The persons making this declaration are the inventors, and are thus qualified to submit this declaration under 37 CFR § 1.131.

FACTS AND DOCUMENTARY EVIDENCE

To establish the date of completion of the invention of this patent application, copies of the following documents and supporting statements are submitted as evidence:

Documents

REVISED EXHIBIT 5: Chart of currently pending independent claim limitations that shows documentation for each claim limitation.

Supporting statements

1. Each claim limitation in Exhibit 5 is supported by documentation that is dated prior to October 20, 2000. Text portions T1-T6 (there is no T2) referred to in Exhibit 5 correspond to respectively labeled text portions in Exhibits 2 and 3 of the originally filed § 1.131 Declaration.

2. The beta and commercial version of ActivePrivacy both contained all of the functionality of the claim limitations shown in Exhibit 5. General descriptions of such functionality are given in Exhibits 2 and 3 of the originally filed § 1.131 Declaration.

From the attached documents and the supporting statements, and the documents and supporting statement in the originally filed § 1.131 Declaration, we submit that it has been established that the invention in this application was made prior to October 20, 2000, which is the earliest possible effective date of Buck.

TIME OF PRESENTATION OF THE DECLARATION

This declaration is submitted prior to final rejection.

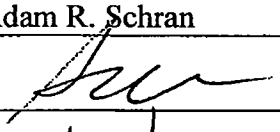
B2

DECLARATION

As a person signing below:

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

SIGNATURES

Full name of first or sole inventor	Adam R. Schran
Inventor's Signature	
Date	10/31/2006
Residence	Philadelphia, Pennsylvania
Citizenship	United States of America
Post Office Address	217 Church Street, #4, Philadelphia, Pennsylvania 19147
Full name of second joint inventor	Robert E. Darlington
Inventor's Signature	
Date	
Residence	Los Alamos, New Mexico
Citizenship	United States of America
Post Office Address	3260-B Orange Street, Los Alamos, New Mexico 87544

B3

DECLARATION

As a person signing below:

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

SIGNATURES

Full name of first or sole inventor: Adam R. Schran

Inventor's Signature: _____

Date: _____

Residence: Philadelphia, Pennsylvania

Citizenship: United States of America

Post Office Address: 217 Church Street, #4, Philadelphia, Pennsylvania 19147

Full name of second joint inventor: Robert E. Darlington

Inventor's Signature: [signature]

Date: 11/4/2006

Residence: Los Alamos, New Mexico

Citizenship: United States of America

Post Office Address: 3260-B Orange Street, Los Alamos, New Mexico 87544

B4

EXHIBIT 5 of "Supplemental Declaration of Prior Invention..."
(Application No. 09/820,054)

Chart of independent claim limitations that shows documentation for each claim limitation

Text of independent claims	Exhibit(s) that support claim limitations
1. A method of screening cookie files in a client machine, wherein a cookie file includes a cookie file source, the method comprising	
(a) receiving, at a server, a request from a subscriber to send a list of cookie file sources to the client machine;	Exhibit 2: T1 Exhibit 3: T1
(b) downloading the list of cookie file sources from the server to the client machine; and	Exhibit 2: T1 Exhibit 3: T1
(c) using the downloaded list of cookie file sources to detect cookie files received at the client machine from cookie file sources on the downloaded list by comparing the cookie file source of any received cookie file to the cookie file sources on the downloaded list.	Exhibit 2: T3 Exhibit 3: T3
16.	Same as claim 1

Text of independent claims	Exhibit(s) that support claim limitations
7. A method of creating a composite list of cookie file sources in a client machine, the method comprising:	
(a) creating a first exception list including the identity of cookie file sources that are permitted to store cookie files in the client machine, wherein a cookie file includes a cookie file source;	Exhibit 2: T4 Exhibit 3: T4
(b) creating a second exception list including the identity of cookie file sources that are not permitted to store cookie files in the client machine;	Exhibit 2: T5 Exhibit 3: T5
(c) receiving at the client machine, from a service provider, a master list of cookie file sources; and	Exhibit 2: T1 Exhibit 3: T1
(d) modifying the master list in accordance with the first and	Exhibit 2: T6

B 57

second exception lists, wherein the composite list is the modified master list.	Exhibit 3: T6
22.	Same as claim 7

Text of independent claims	Exhibit(s) that support claim limitations
12. A method of creating a composite list of cookie file sources in a client machine, the method comprising:	
(a) receiving at the client machine, from a service provider, a master list of cookie file sources;	Exhibit 2: T1 Exhibit 3: T1
(b) deleting cookie file sources from the master list that correspond to one or more trusted cookie file sources listed in the client machine; and	Exhibit 2: T4, T6 Exhibit 3: T4, T6
(c) adding cookie file sources to the master list that correspond to one or more untrusted cookie file sources listed in the client machine, wherein the composite list is the master list as modified by any additions and deletions of trusted and untrusted cookie file sources.	Exhibit 2: T5, T6 Exhibit 3: T5, T6
27.	Same as claim 12

X. APPENDIX OF RELATED DECISIONS

None.

XI. OTHER MATERIAL THAT APPELLANT CONSIDERS NECESSARY OR DESIRABLE

None.

Respectively submitted,

Adam R. Schran *et al.*

February 4, 2009 By: Clark Jablon
(Date)

CLARK A. JABLON
Registration No. 35,039
PANITCH SCHWARZE BELISARIO & NADEL LLP
One Commerce Square
2005 Market Street, Suite 2200
Philadelphia, PA 19103-7013
Telephone: 215-965-1330
Direct Dial: 215-965-1293